

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-222426

(43)Date of publication of application : 21.08.1998

(51)Int.Cl.

G06F 12/14

(21)Application number : 09-021867

(71)Applicant : YOKOGAWA DENSHI KIKI KK

(22)Date of filing : 04.02.1997

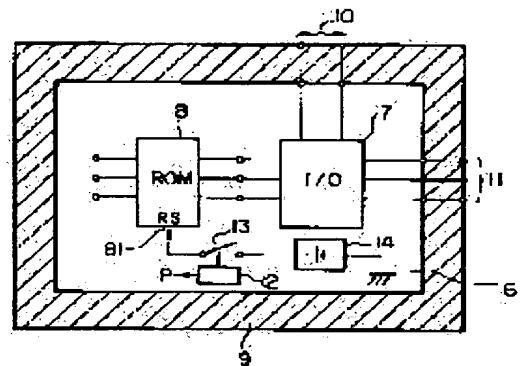
(72)Inventor : OKUBO AKIRA
SUENAGA SHUGO

(54) PROTECTION DEVICE FOR ELECTRONIC INFORMATION

(57)Abstract:

PROBLEM TO BE SOLVED: To surely prevent the forgery crime of a card by detecting the destruction of a container means for the purpose of illegal access and erasing holding information of a semiconductor based on the output.

SOLUTION: A pressure sensor 12 provided in a container 9 detects the change of pressure P in the container owing to destruction and operates a switch 13 provided in the container 9. Voltage is supplied to the reset terminal 81 of ROM 8 with the operation of the switch 13 and electronic information is completely reset/erased by power feeding. When the container 9 is destroyed for the purpose of the illegal access of electronic information in ROM 8, electronic information is erased by the operation of the pressure sensor 12. Thus, the possibility of illegal copy is surely prevented. Namely, electronic information of ROM 8 is erased and ROM 8 itself is destroyed without fail with the destruction of the container 9. Thus, the illegal access of electronic information can surely be prevented.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(11)特許出願公開番号

特開平10-222426

(43)公開日 平成10年(1998)8月21日

FI

3 2 0 D

審査請求 未請求 請求項の数2 O L (全 4 頁)

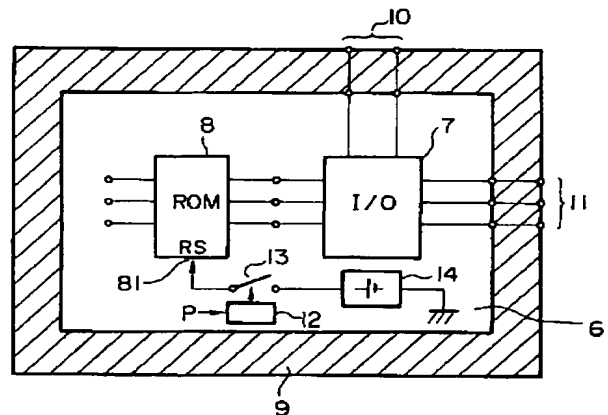
(74) 代理人 弁理士 志賀 正武 (外2名)

(54) 【発明の名称】 電子情報の保護装置

(57) 【要約】

【課題】 半導体に格納された電子情報への不法アクセスを確実に防止する保護装置を提供すること。

【解決手段】 不法アクセスから保護すべき電子情報を保持したROM8を含む電子回路は、容器16に密封収納されている。不法アクセスの目的でこの容器が破壊された時に圧力センサー12による破壊検知手段が作動し、その出力に基づいて電子情報がリセット消去され、又は破壊検知手段の出力に基づいてROM8自身が物理的に破壊される。



【特許請求の範囲】

【請求項1】 不法アクセスから保護すべき電子情報を保持した半導体を含む電子回路を密封する容器手段と、上記不法アクセスの目的で上記容器手段が破壊されたことを検知する破壊検知手段と、この破壊検知手段の出力に基づいて上記半導体の保持情報を消去する手段と、を具備した電子情報の保護装置。

【請求項2】 不法アクセスから保護すべき電子情報を保持した半導体を含む電子回路を密封する容器手段と、上記不法アクセスの目的で上記容器手段が破壊されたことを検知する破壊検知手段と、この破壊検知手段の出力に基づいて上記半導体を物理的に破壊する手段と、を具備した電子情報の保護装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、半導体に保持された重要情報を不法アクセスから確実に保護する装置に関する。

【0002】

【従来の技術】図3により、プリペイドカードによる品物（例えばパチンコの玉）の自動販売システムの一例を説明する。符号1はあらかじめ金融機関などから所定の金額支払いで消費者が購入するプリペイドカードである。符号2はマンマシンインターフェイスであり、カード情報の読み取り、書き込み、購入要求（矢印A）の入力受付、表示等の機能を有する。

【0003】符号3はマンマシンインターフェイス2と情報交換を行う制御装置であり、プリペイドカード1の真偽判断、残高確認、購入要求内容Aの判断を行い、販売装置4に対し購入要求に基づく品物5を出力させる指令を発信すると共に、マンマシンインターフェイス2を介してプリペイドカード1に対して残高精算の書き込み処理、精算表示を行う。

【0004】符号6は制御装置3の主要部を構成する電子回路基板であり、基板上には入出力電子回路（I/O）7及びこの入出力電子回路と接続されて情報交換を行う、プログラムやデータ等のソフトウェア（電子情報）を格納したROM（リードオンリーメモリ）8が搭載されている。

【0005】符号9は入出力電子回路7を介して接続される上位のネットワークであり、カードによる取引内容を収集し、直接又はセンターコンピュータを介してカードを販売した金融機関と交信し、品物の販売に対する金銭精算が行われる。

【0006】

【発明が解決しようとする課題】このようなシステムにおいては、ROM8に格納された電子情報を知ることにより、カードを偽造（正規のカードと同一のもの）する

ことが技術的に可能である。このような不法アクセスを防止する手段としては、暗号手段によるガードが一般であるが、特殊な装置によればこれを破ることができるため、現状ではカードの偽造犯罪を確実に防止する有効手段がない、という点が問題となっている。本発明はこのような事情に鑑みてなされたもので、ROMへの不法アクセスに対し、ROMを収納した容器を破壊することにより、カードの偽造犯罪を確実に防止することを目的とする。

【0007】

【課題を解決するための手段】本発明は、上記問題を解決する目的でなされたもので、その特徴の第1は、不法アクセスから保護すべき電子情報を保持した半導体を含む電子回路を密封する容器手段と、上記不法アクセスの目的で上記容器手段が破壊されたことを検知する破壊検知手段と、この破壊検知手段の出力に基づいて上記半導体の保持情報を消去する手段とを具備せしめた点にある。さらにその特徴の第2は、不法アクセスから保護すべき電子情報を保持した半導体を含む電子回路を密封する容器手段と、上記不法アクセスの目的で上記容器手段が破壊されたことを検知する破壊検知手段と、この破壊検知手段の出力に基づいて上記半導体を物理的に破壊する手段とを具備せしめた点にある。

【0008】上記の構成によれば、不法アクセスから保護すべき電子情報を保持した半導体を含む電子回路は密封容器に収納されており、不法アクセスの目的でこの容器が破壊された時に破壊検知手段が作動し、その出力に基づいて半導体の保持情報が消去され、又は破壊検知手段の出力に基づいて半導体が物理的に破壊される。

【0009】

【発明の実施の形態】以下、図面に基づき、本発明の一実施形態による電子情報の保護装置について更に詳しく説明する。図1は本発明の一実施形態による電子情報の保護装置を示す平面図であり、図3のシステムで説明した構成要素と同一要素については同一符号を付して表示する。

【0010】符号16は電子回路基板6を密封して収納する容器であり、容器内は空気又はガスにより高圧又は負圧に維持されている。符号10はこの容器16側部に形成されたハーメチックシールされた電源供給端子、符号11は同じくハーメチックシールされた入出力端子であり、これら端子を介して入出力電子回路7は外部環境と電気的に接続される。

【0011】符号12は容器16内に設けられた圧力センサーであり、破壊による容器内圧力Pの変化を検出し、同じく容器16内に設けたスイッチ13を作動させる。

【0012】符号14はさらに容器16内に設けられた電池であり、寿命の長いリチウム電池等で実現される。この電池電圧は、スイッチ13の作動でROM8の

リセット端子81に供給され、この給電により電子情報が完全にリセット消去される。

【0013】このような構成により、ROM8内の電子情報の不法アクセスを目的に容器16が破壊された場合には、圧力センサー12の作動により電子情報は消去せしめられるので、不法にコピーされる可能性は確実に防止される。

【0014】図2は、第二の実施形態による電子情報の保護装置の、圧力センサー及びスイッチを半導体素子で実現した回路を示す図であり、可変インピーダンス型の圧力センサー12と抵抗15による分圧回路を介して電池14の電圧を電界効果トランジスタによるスイッチ13のゲートに供給してドレイン・ソース間を開閉制御する。

【0015】このスイッチ13は、ROM8のリセット端子（逆相）と接地間に接続され、圧力センサー12の作動でオンに制御されるとリセット端子81が接地電位となり、ROM8内の電子情報が完全にリセット消去される。

【0016】図1、図2の例では、容器の破壊を検出する手段として圧力変化に着目し、スイッチの作動でROM8の電子情報をリセットさせているが、保護の手段としてはROM8自身を物理的に破壊する手段を取ることが可能である。

【0017】例えばROM8の上面に燐等を塗布し、容器16内を真空に保持して密封しておけば、容器16の破壊により空気が混入して燐と化学反応を起こし、燃えることにより物理的破壊を実現する。この場合の燃焼破壊規模は、ROM8のみの局部的とし、その他の要素に*

* 火災が波及しないように安全設計される。

【0018】他の破壊手段としては、圧力変化によるスイッチの作動で微量の火薬を点火してROM8を局部的に焼却破壊する方法も可能である。

【0019】

【発明の効果】以上説明した通り、本発明の保護装置においては、ROMへの不法アクセスには、これを密封収納した容器の破壊が必要であり、容器の破壊に伴い必ずROMの電子情報の消去またはROM自身の破壊が行われるので、電子情報の不法アクセスを確実に防ぐことが可能となる。

【図面の簡単な説明】

【図1】 本発明の第一実施形態による電子情報の保護装置の平面図である。

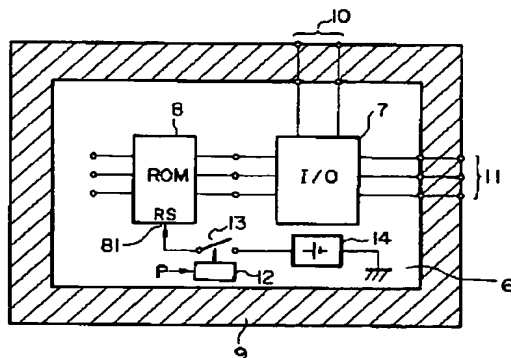
【図2】 本発明の他実施形態による電子情報の保護装置の圧力センサー、スイッチを示す回路図である。

【図3】 プリペイドカードによる販売システムの一例を示すブロック線図である。

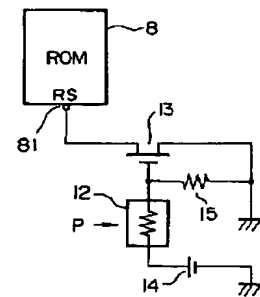
【符号の説明】

- 6 電子回路基板
- 7 入出力電子回路（I/O）
- 8 ROM（リードオンリーメモリ）
- 9 容器
- 10 ハーメチックシール端子
- 11 ハーメチックシール端子
- 12 圧力センサー
- 13 スイッチ
- 14 電池

【図1】



【図2】



(4)

特開平10-222426

【図3】

